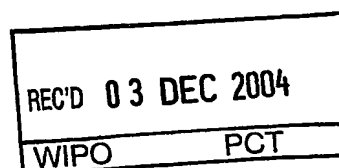


06 OCT. 2004



BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 29 SEP. 2004

DOCUMENT DE PRIORITÉ

PRÉSENTÉ OU TRANSMIS
CONFORMÉMENT À LA
RÈGLE 17.1.a) OU b)

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

Martine PLANCHE

BEST AVAILABLE COPY

INSTITUT
NATIONAL DE
LA PROPRIÉTÉ
INDUSTRIELLE

SIEGE
26 bis, rue de Saint-Petersbourg
75800 PARIS cedex 08
Téléphone : 33 (0)1 53 04 53 04
Télécopie : 33 (0)1 53 04 45 23
www.inpi.fr



26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 33 (1) 53 04 53 04 Télécopie : 33 (1) 42 94 86 54

BREVET D'INVENTION CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI



REQUÊTE EN DÉLIVRANCE page 1/2



Cet imprimé est à remplir lisiblement à l'encre noire

DB 540 e W / 210502

REMISE DES PIÈCES DATE 26 SEPT 2003 LIEU 75 INPI PARIS F N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI 0311350 DATE DE DÉPÔT ATTRIBUÉE PAR L'INPI 26 SEP. 2003		NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE Monsieur SAINT-MARC Christophe Cabinet LE GUEN MAILLET 5, place Newquay B.P. 70250 35802 DINARD CEDEX	
Vos références pour ce dossier (facultatif) 10434			
Confirmation d'un dépôt par télécopie		<input checked="" type="checkbox"/> N° attribué par l'INPI à la télécopie	
2 NATURE DE LA DEMANDE		Cochez l'une des 4 cases suivantes	
Demande de brevet		<input checked="" type="checkbox"/>	
Demande de certificat d'utilité		<input type="checkbox"/>	
Demande divisionnaire		<input type="checkbox"/>	
Demande de brevet initiale		N°	Date
ou demande de certificat d'utilité initiale		N°	Date
Transformation d'une demande de brevet européen		<input type="checkbox"/>	Date
Demande de brevet initiale		N°	Date
3 TITRE DE L'INVENTION (200 caractères ou espaces maximum) Système de télécommunication mettant en oeuvre une résolution de noms de domaine sécurisée			
4 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE FRANÇAISE		Pays ou organisation Date N° Pays ou organisation Date N° Pays ou organisation Date N° <input type="checkbox"/> S'il y a d'autres priorités, cochez la case et utilisez l'imprimé «Suite»	
5 DEMANDEUR (Cochez l'une des 2 cases)		<input checked="" type="checkbox"/> Personne morale <input type="checkbox"/> Personne physique	
Nom ou dénomination sociale		FRANCE TELECOM	
Prénoms			
Forme juridique		S.A.	
N° SIREN		3 8 0 1 2 9 8 6 6	
Code APE-NAF			
Domicile ou siège	Rue	6, place d'Alleray	
	Code postal et ville	75 015 PARIS	
	Pays	FRANCE	
Nationalité		Française	
N° de téléphone (facultatif)		N° de télécopie (facultatif)	
Adresse électronique (facultatif)			
<input type="checkbox"/> S'il y a plus d'un demandeur, cochez la case et utilisez l'imprimé «Suite»			

Remplir impérativement la 2^{ème} page



BREVET D'INVENTION CERTIFICAT D'UTILITÉ

REQUÊTE EN DÉLIVRANCE
page 2/2

BR2

REMISE DES PIÈCES DATE 26 SEPT 2003 LIEU 75 INPI PARIS F N° D'ENREGISTREMENT 0311350 NATIONAL ATTRIBUÉ PAR L'INPI		Réservé à l'INPI	DB 540 W / 210502
6 MANDATAIRE (s) (facultatif)			
Nom		SAINT-MARC	
Prénom		Christophe	
Cabinet ou Société		Cabinet LE GUEN MAILLET	
N° de pouvoir permanent et/ou de lien contractuel			
Adresse	Rue	5, place Newquay B.P. 70250	
	Code postal et ville	13 5 18 10 12 DINARD	
	Pays	FRANCE	
N° de téléphone (facultatif)		02 99 46 55 19	
N° de télécopie (facultatif)		02 99 46 41 80	
Adresse électronique (facultatif)			
7 INVENTEUR (S) Les inventeurs sont nécessairement des personnes physiques			
Les demandeurs et les inventeurs sont les mêmes personnes		<input type="checkbox"/> Oui <input checked="" type="checkbox"/> Non : Dans ce cas remplir le formulaire de Désignation d'inventeur(s)	
8 RAPPORT DE RECHERCHE Uniquement pour une demande de brevet (y compris division et transformation)			
Établissement immédiat ou établissement différé		<input checked="" type="checkbox"/> <input type="checkbox"/>	
Paiement échelonné de la redevance (en deux versements)		Uniquement pour les personnes physiques effectuant elles-mêmes leur propre dépôt <input type="checkbox"/> Oui <input type="checkbox"/> Non	
9 RÉDUCTION DU TAUX DES REDEVANCES		Uniquement pour les personnes physiques <input type="checkbox"/> Requête pour la première fois pour cette invention (joindre un avis de non-imposition) <input type="checkbox"/> Obtenue antérieurement à ce dépôt pour cette invention (joindre une copie de la décision d'admission à l'assistance gratuite ou indiquer sa référence) : AG [] [] [] [] []	
10 SÉQUENCES DE NUCLEOTIDES ET/OU D'ACIDES AMINÉS		<input type="checkbox"/> Cochez la case si la description contient une liste de séquences	
Le support électronique de données est joint La déclaration de conformité de la liste de séquences sur support papier avec le support électronique de données est jointe		<input type="checkbox"/> <input type="checkbox"/>	
Si vous avez utilisé l'imprimé «Suite», indiquez le nombre de pages jointes			
11 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE (Nom et qualité du signataire) SAINT-MARC Christophe 01-1000		VISA DE LA PRÉFECTURE OU DE L'INPI	

La présente invention concerne un système de télécommunication incluant une base de données destinée à être reliée à au moins un terminal au moyen d'un réseau de communication, laquelle base de données incluant des données associées à au moins un nom de domaine.

5 De telles bases de données sont couramment utilisées dans des systèmes de télécommunication mettant en œuvre un ou plusieurs réseaux maillés publics, systèmes dans lesquels un terminal connaissant un nom de domaine d'un interlocuteur donné interrogera une base de données au moyen de ce nom de domaine pour en
10 obtenir une adresse de protocole courante qui peut être amenée à varier dans le temps, par exemple une adresse IP si un réseau Internet est mis en œuvre. A cet effet, la base de données tient à jour une table de correspondance entre divers noms de domaines et des adresses de protocole associées à ces noms de domaine. Un tel service de fourniture d'adresses de protocole courantes associées à des noms de domaine connus de terminaux appelants est connu de l'homme du métier sous l'abréviation DNS de
15 l'expression anglaise "Domain Name Service", la base de données étant en principe hébergée au sein d'un serveur couramment appelé serveur DNS et réalisant, en mettant en correspondance un nom de domaine et une adresses de protocole associée à ce nom de domaine, une opération appelée résolution.

Dans certaines applications, des données confidentielles pourront être associées
20 à un nom de domaine figurant dans la base de données hébergée dans le serveur DNS. De telles données confidentielles pourront simplement être constituées par des adresses de protocole particulières qui doivent être tenues secrètes et ne pourront être communiquées qu'à une population restreinte préalablement définie. Les données confidentielles pourront également être constituées par des informations de profil
25 propres au détenteur d'un site identifié par le nom de domaine considéré, ou par des informations techniques propre au site lui-même.

Or, dans l'état actuel de la technique, le serveur DNS, qui fonctionne à la manière d'une mémoire associative adressable au moyen du nom de domaine, n'opère aucun filtrage des informations qu'il restitue en réponse à une requête identifiant un

nom de domaine donné, de sorte que le respect du caractère confidentiel de certaines données n'est en aucun cas garanti.

L'un des buts de l'invention est de permettre la réalisation d'un service de fourniture d'adresses de protocole qui assure un respect du caractère confidentiel que
5 pourraient revêtir certaines données mémorisées dans une base de données en correspondance avec un ou plusieurs noms de domaine associés auxdites adresses de protocole.

En effet, un système de télécommunication conforme au paragraphe introductif est caractérisé selon l'invention en ce que la base de données inclut un serveur dit de
10 référence, destiné à contenir des données associées à au moins un nom de domaine, et au moins un premier et un deuxième serveur auxiliaire destinés à contenir des données préalablement enregistrées au sein du serveur de référence et respectivement munies d'un premier et d'un deuxième degré de confidentialité, au moins l'un des premier et deuxième serveurs auxiliaires étant muni de moyens d'identification pour interdire
15 tout accès aux données qu'il contient à des terminaux ne possédant pas d'autorisation d'accès compatible avec le degré de confidentialité attribué aux données contenues dans ce serveur auxiliaire.

L'invention permet d'exercer un contrôle sur les conditions de communication au public des informations contenues dans la base de données, en séparant les données
20 initialement contenues dans le serveur de référence en au moins deux groupes de données présentant des degrés de confidentialité différents, lesquels groupes étant respectivement destinés à être contenus dans des serveurs auxiliaires distincts et accessibles à des populations préalablement définies, qui pourront être spécifiques à chaque serveur auxiliaire et différentes d'un serveur auxiliaire à l'autre.

25 La base de données sera avantageusement munie de moyens de duplication des données contenues dans le serveur de référence vers les premier et deuxième serveurs auxiliaires en fonction des degrés de confidentialité attribués auxdites données.

La duplication vers les serveurs auxiliaires des informations contenues dans le serveur de référence permettra une consultation de ces informations au niveau des

serveurs auxiliaires, en autorisant la conservation d'une version de sauvegarde de ces informations au sein du serveur de référence.

Les premier et deuxième serveurs auxiliaires seront avantageusement munis de moyens d'identification pour interdire tout accès aux données contenues dans les premier et deuxième serveurs auxiliaires à des terminaux ne possédant pas d'autorisations d'accès respectivement compatibles avec les premier et deuxième degrés de confidentialité.

Les moyens d'identification constituent un moyen simple de restriction d'accès aux informations contenues dans un serveur donné, puisqu'ils imposent à chaque terminal ayant requis l'accès de faire la preuve de son droit d'accès, et dispensent ainsi le serveur de toute recherche d'informations supplémentaires en vue d'établir l'existence ou l'inexistence de ce droit.

D'autres moyens de restriction d'accès, tels des moyens de localisation du terminal ayant émis une requête d'accès, pourront bien sûr être utilisés pour interdire un accès à des données à des terminaux ne possédant pas d'autorisation d'accès compatible avec le degré de confidentialité attribué auxdites données, la compatibilité étant de nature géographique dans cet autre exemple.

Le serveur de référence pourra être inaccessible, en lecture comme en écriture, à tous les terminaux extérieurs, hormis à certains équipements de contrôle appartenant à un gestionnaire du système qui doit être capable de modifier, de supprimer ou d'ajouter de manière dynamique des adresses de protocole, ainsi éventuellement que des données confidentielles liées à des noms de domaine inclus dans la base de données. Une telle inaccessibilité garantit une certaine intégrité des données contenues dans le serveur de référence, que ces données soient ou non confidentielles.

Afin de conférer à la base de données conforme à l'invention un degré de liberté supplémentaire pour son fonctionnement, on pourra cependant autoriser un accès en lecture seulement aux données contenues dans le serveur de référence. A cet effet, le serveur de référence sera muni de moyens d'identification pour interdire toute lecture des données contenues dans ledit serveur de référence depuis des terminaux ne

possédant pas d'autorisation d'accès compatible avec un troisième degré de confidentialité.

Pour préserver au maximum l'intégrité des données contenues dans le serveur de référence auxquelles un accès en lecture est ainsi rendu possible, le troisième degré de confidentialité aura un effet restrictif supérieur aux effets restrictifs produits par les premier et deuxième degrés de confidentialité.

La population apte à lire directement les informations contenues dans le serveur de référence sera ainsi moins nombreuse que les populations autorisées à consulter les serveurs auxiliaires.

Dans un même souci de préservation de l'intégrité des données qu'il est destiné à contenir, le serveur de référence sera de préférence muni de moyens d'identification pour interdire toute écriture de données dans ledit serveur de référence depuis un terminal ne possédant pas d'autorisation d'accès compatible avec un degré de confidentialité supérieur ayant un effet restrictif supérieur aux effets restrictifs produits par tous les autres degrés de confidentialité attribués aux données contenues dans le serveur de référence et dans les serveurs auxiliaires.

L'invention concerne également, en tant que moyen essentiel à sa mise en œuvre, un dispositif de mémorisation d'informations incluant un serveur dit de référence, et au moins un premier et un deuxième serveur auxiliaire destinés à contenir des données préalablement enregistrées au sein du serveur de référence et respectivement munies d'un premier et d'un deuxième degré de confidentialité, au moins l'un des premier et deuxième serveurs auxiliaires étant muni de moyens d'identification pour interdire tout accès aux données qu'ils contiennent à des requérants ne possédant pas d'autorisation d'accès compatible avec le degré de confidentialité attribué aux données contenues dans ce serveur auxiliaire.

Les caractéristiques de l'invention mentionnées ci-dessus, ainsi que d'autres, apparaîtront plus clairement à la lecture de la description suivante d'un exemple de réalisation, ladite description étant faite en relation avec la Fig.1 qui est un schéma fonctionnel représentant, sous une forme simplifiée, un système de télécommunication dans lequel l'invention est mise en œuvre.

Ce système de télécommunication inclut une base de données DBS destinée à être reliée à au moins un terminal TER0, TER1 ou TER2 au moyen d'un réseau de communication, par exemple un réseau maillé de type Internet. Dans ce mode de réalisation particulier de l'invention, la base de données DBS inclut un serveur de
 5 référence REFS destiné à contenir des données associées à au moins un nom de domaine, et un premier et un deuxième serveur auxiliaire CFS et PBS destinés à contenir des données préalablement enregistrées au sein du serveur de référence et respectivement munies d'un premier et d'un deuxième degré de confidentialité.

A cet effet, chacun des premier et deuxième serveurs auxiliaires CFS et PBS est
 10 muni de moyens d'identification, respectivement IDMC et IDMP, pour interdire tout accès aux données qu'il contient à des terminaux ne possédant pas d'autorisation d'accès compatible avec le degré de confidentialité attribué aux données CONFD ou PUBD contenues dans ce serveur auxiliaire CFS ou PBS.

Les premier et deuxième degrés de confidentialité seront en principe choisis de
 15 telle sorte qu'ils définiront deux populations différentes, la population autorisée à accéder aux données confidentielles CONFD contenues dans le premier serveur auxiliaire CFS étant de par ce choix de taille très inférieure à la population autorisée à accéder aux données publiques PUBD contenues dans le deuxième serveur auxiliaire PBS.

Dans un cas simplifié d'un tel mode de mise en œuvre de l'invention, seules les
 20 données CONFD contenues dans le premier serveur auxiliaire CFS seront des données confidentielles, par opposition aux données PUBD contenues dans le deuxième serveur auxiliaire PBS qui seront des données publiques. Dans un tel cas simplifié, les moyens d'identification IDMP mentionnés ci-dessus pourront être inexistantes ou
 25 simplement aptes à contrôler un respect de conditions de forme auxquelles seraient assujetties des requêtes en lecture RRq(PUBD) des données publiques PUBD contenues dans le deuxième serveur auxiliaire PBS.

Lorsqu'un terminal TER2 souhaitera consulter des données contenues dans le premier serveur auxiliaire CFS, ledit terminal enverra tout d'abord une requête
 30 RqAIP(CFS) à un serveur racine RTS aux fins de se voir communiquer l'adresse de

protocole AIP(CFS) de ce premier serveur auxiliaire CFS. Cette requête RqAIP(CFS) sera usuellement accompagnée d'un identifiant ID2 de ce terminal TER2. Le terminal TER2 pourra ensuite émettre à destination de cette adresse de protocole AIP(CFS) une requête de lecture RRq(CONFD) d'informations CONFD identifiées par le nom de domaine qui leur est associé et qui est connu du terminal TER2. Cette requête RRq(CONFD) sera accompagnée de l'identifiant ID2 et parviendra au premier serveur auxiliaire CFS *via* les moyens d'identification IDMC dont il est muni. Si l'identifiant ID2 identifie le terminal TER2 comme appartenant à la population autorisée à accéder aux données CONFD munies du premier degré de confidentialité et considérées comme confidentielles dans cet exemple, les données CONFD requises seront transmises en retour au terminal TER2. Dans le cas contraire, les moyens d'identification IDMC pourront émettre vers le terminal TER2 un avis d'irrecevabilité, ou simplement mettre fin à la connexion entre le terminal TER2 et le premier serveur auxiliaire CFS. Les requêtes et messages décrits précédemment transiteront avantageusement *via* le réseau Internet, auquel cas les adresses de protocole seront des adresses IP.

Lorsque le terminal TER2 souhaitera consulter des données contenues dans le deuxième serveur auxiliaire PBS, ledit terminal enverra tout d'abord une requête RqAIP(PBS), accompagnée de l'identifiant ID2, au serveur racine RTS aux fins de se voir communiquer l'adresse de protocole AIP(PBS) de ce deuxième serveur auxiliaire PBS. Le terminal TER2 pourra ensuite émettre à destination de cette adresse de protocole AIP(PBS) une requête de lecture RRq(PUBD) d'informations PUBD identifiées par le nom de domaine qui leur est associé et qui est connu du terminal TER2. Cette requête RRq(PUBD) parviendra au deuxième serveur auxiliaire PBS *via* les moyens d'identification IDMP dont il est muni. Les données contenues dans le deuxième serveur auxiliaire PBS étant publiques dans le cas simplifié décrit ici, l'identifiant ID2 du terminal T2 n'est pas nécessaire pour obtenir un accès à ces données PUBD, qui seront automatiquement transmises en retour au terminal TER2, à moins que la requête de lecture RRq(PUBD) ne présente un vice de forme qui sera détecté par les moyens d'identification IDMP. Tout terminal formulant une requête de

lecture de données PUBD contenues dans le deuxième serveur auxiliaire PBS est ainsi présumé posséder une autorisation d'accès compatible avec le degré de confidentialité très faible qui est attribué dans cet exemple auxdites données PUBD.

Chacun des premier et deuxième serveurs auxiliaires CFS et PBS pourra être
 5 construit selon une architecture maître-esclave bien connue de l'homme du métier, et inclure ainsi un ou plusieurs serveurs esclaves non-représentés ici et agencés en parallèle sous la dépendance d'un unique serveur maître qui jouira d'une compétence exclusive pour exécuter une requête en écriture dans l'un des serveurs esclaves qu'il contrôle.

10 Dans le mode de mise en œuvre particulier de l'invention décrit ici, la base de données DBS est munie de moyens de duplication SPLM des données CONFD, PUBD contenues dans le serveur de référence REFS vers les premier et deuxième serveurs auxiliaires CFS et PBS en fonction des degrés de confidentialité attribués auxdites données.

15 La duplication vers les serveurs auxiliaires CFS et PBS des données CONFD, PUBD contenues dans le serveur de référence REFS permettra une consultation de ces données CONFD, PUBD au niveau des serveurs auxiliaires CFS et PBS, en autorisant la conservation d'une version de sauvegarde de ces données au sein du serveur de référence REFS.

20 Pour exécuter une telle répartition des copies des données CONFD, PUBD, les moyens de duplication SPLM pourront mettre en œuvre une fonction de répartition destinée à analyser un champ de répartition associé à chaque donnée et destiné à contenir une valeur représentative du degré de confidentialité attribué à ladite donnée. Ainsi, dans le cas simplifié décrit ci-dessus où les données sont considérées soit
 25 comme publiques, soit comme confidentielles, le champ de répartition pourra par exemple ne contenir qu'un seul bit égal à "0" s'il est associé à une donnée publique PUBD ou à "1" dans le cas d'une donnée confidentielle CONFD.

Dans le mode de réalisation particulier de l'invention décrit ici, un accès supplémentaire, mais uniquement en lecture, aux données contenues dans le serveur
 30 de référence REFS a été prévu afin de conférer à la base de données DBS un degré de

liberté supplémentaire pour son fonctionnement. A cet effet, le serveur de référence REFS est muni de moyens d'identification IDMR pour interdire toute lecture des données contenues dans ledit serveur de référence REFS depuis des terminaux ne possédant pas d'autorisation d'accès compatible avec un troisième degré de confidentialité.

Pour préserver au maximum l'intégrité des données contenues dans le serveur de référence REFS auxquelles un accès en lecture est ainsi rendu possible, le troisième degré de confidentialité aura un effet restrictif supérieur aux effets restrictifs produits par les premier et deuxième degrés de confidentialité. La population apte à lire directement les informations contenues dans le serveur de référence REFS sera ainsi moins nombreuse que les populations autorisées à consulter les serveurs auxiliaires CFS et PBS.

Lorsqu'un terminal TER1 souhaitera consulter des données contenues dans le serveur de référence REFS, ledit terminal TER1 enverra tout d'abord une requête de lecture RqAIP(REFS) au serveur racine RTS aux fins de se voir communiquer l'adresse de protocole AIP(REFS) de ce serveur de référence REFS. Cette requête de lecture RqAIP(REFS) sera usuellement accompagnée de l'identifiant ID1 de ce terminal TER1. Le terminal TER1 pourra ensuite émettre à destination de cette adresse de protocole AIP(REFS) une requête de lecture RRq(CONFD) d'informations CONFD identifiées par le nom de domaine qui leur est associé et qui est connu du terminal TER1. Cette requête RRq(CONFD) sera accompagnée de l'identifiant ID1 et parviendra au serveur de référence REFS *via* des moyens d'identification IDMR dont il est muni. Si l'identifiant ID1 identifie le terminal TER1 comme appartenant à la population munie du troisième degré de confidentialité, les données CONFD requises seront transmises en retour au terminal TER1. Dans le cas contraire, les moyens d'identification IDMR pourront émettre vers le terminal TER1 un avis d'irrecevabilité, ou simplement mettre fin à la connexion entre le terminal TER1 et le serveur de référence REFS.

La procédure décrite ci-dessus est également applicable à la lecture directe de données publiques contenues dans le serveur de référence REFS.

Dans un souci constant de préservation de l'intégrité des données qu'il est destiné à contenir, le serveur de référence REFS est ici muni de moyens d'identification IDMW pour interdire toute écriture de données dans ledit serveur de référence REFS depuis un terminal TER0 ne possédant pas d'autorisation d'accès compatible avec un degré de confidentialité ayant un effet restrictif supérieur aux effets restrictifs produits par tous les autres degrés de confidentialité attribués aux données contenues dans le serveur de référence et dans les serveurs auxiliaires.

La population apte à écrire ou à modifier des données dans le serveur de référence REFS sera ainsi encore moins nombreuse que les populations exclusivement autorisées à lire directement des informations contenues dans le serveur de référence REFS, et, *a fortiori*, bien moins nombreuse que les populations autorisées à consulter les serveurs auxiliaires CFS et PBS.

Lorsqu'un terminal TER0 souhaitera écrire des données dans le serveur de référence REFS ou modifier des données contenues dans le serveur de référence REFS, ledit terminal TER0 enverra tout d'abord une requête RqAIP(REFS) au serveur racine RTS aux fins de se voir communiquer l'adresse de protocole AIP(REFS) de ce serveur de référence REFS. Cette requête RqAIP(REFS) sera usuellement accompagnée de l'identifiant ID0 de ce terminal TER0. Le terminal TER0 pourra ensuite émettre à destination de cette adresse de protocole AIP(REFS) une requête d'écriture WRq(CONFD, PUBD) d'informations confidentielles ou publiques destinées à être identifiées par un nom de domaine qui leur est associé, laquelle requête d'écriture WRq(CONFD, PUBD) sera accompagnée de l'identifiant ID0 et parviendra au serveur de référence REFS *via* des moyens d'identification supplémentaires IDMW dont il est muni. Si l'identifiant ID0 identifie le terminal TER0 comme appartenant à la population très restreinte autorisée à écrire des données dans le serveur de référence REFS, les données CONFD, PUBD seront inscrites à une adresse spécifiée dans la requête d'écriture WRq(CONFD, PUBD), qui sera représentative du nom de domaine associé aux données CONFD, PUBD. Dans le cas contraire, les moyens d'identification IDMR pourront émettre vers le terminal TER0

un avis d'irrecevabilité, ou simplement mettre fin à la connexion entre le terminal TER0 et le serveur de référence REFS.

L'invention décrite ci-dessus permet donc la réalisation d'un service de fourniture d'adresses de protocole qui assure un respect du caractère confidentiel que
5 pourraient revêtir certaines données CONFD mémorisées dans la base de données DBS en correspondance avec un ou plusieurs noms de domaine associés auxdites adresses de protocole.

REVENDECATIONS

1) Système de télécommunication incluant une base de données destinée à être reliée à au moins un terminal au moyen d'un réseau de communication, laquelle base de données incluant un serveur dit de référence, destiné à contenir des données associées à au moins un nom de domaine, et au moins un premier et un deuxième
 5 serveur auxiliaire destinés à contenir des données préalablement enregistrées au sein du serveur de référence et respectivement munies d'un premier et d'un deuxième degré de confidentialité, au moins l'un des premier et deuxième serveurs auxiliaires étant muni de moyens d'identification pour interdire tout accès aux données qu'il contient à des terminaux ne possédant pas d'autorisation d'accès compatible avec le
 10 degré de confidentialité attribué aux données contenues dans ce serveur auxiliaire.

2) Système de télécommunication selon la revendication 1, caractérisé en ce que la base de données est munie de moyens de duplication des données contenues dans le serveur de référence vers les premier et deuxième serveurs auxiliaires en fonction des degrés de confidentialité attribués auxdites données.

15 3) Système de télécommunication selon l'une des revendications 1 ou 2, caractérisé en ce que les premier et deuxième serveurs auxiliaires sont munis de moyens d'identification pour interdire tout accès aux données contenues dans les premier et deuxième serveurs auxiliaires à des terminaux ne possédant pas d'autorisations d'accès respectivement compatibles avec les premier et deuxième
 20 degrés de confidentialité.

4) Système de télécommunication selon l'une des revendications 1 à 3, caractérisé en ce que le serveur de référence est muni de moyens d'identification pour interdire toute lecture des données contenues dans ledit serveur de référence depuis des terminaux ne possédant pas d'autorisation d'accès compatible avec un troisième
 25 degré de confidentialité.

5) Système de télécommunication selon l'une des revendications 1 à 4, caractérisé en ce que le troisième degré de confidentialité a un effet restrictif supérieur aux effets restrictifs produits par les premier et deuxième degrés de confidentialité.

6) Système de télécommunication selon l'une des revendications 1 à 5, caractérisé en ce que le serveur de référence est muni de moyens d'identification pour interdire toute écriture de données dans ledit serveur de référence depuis un terminal ne possédant pas d'autorisation d'accès compatible avec un degré de confidentialité
5 supérieur ayant un effet restrictif supérieur aux effets restrictifs produits par tous les autres degrés de confidentialité attribués aux données contenues dans le serveur de référence et dans les serveurs auxiliaires.

7) Dispositif de mémorisation d'informations incluant un serveur dit de référence, et au moins un premier et un deuxième serveur auxiliaire destinés à contenir
10 des données préalablement enregistrées au sein du serveur de référence et respectivement munies d'un premier et d'un deuxième degré de confidentialité, au moins l'un des premier et deuxième serveurs auxiliaires étant muni de moyens d'identification pour interdire tout accès aux données qu'ils contiennent à des requérants ne possédant pas d'autorisation d'accès compatible avec le degré de confidentialité
15 attribué aux données contenues dans ce serveur auxiliaire.

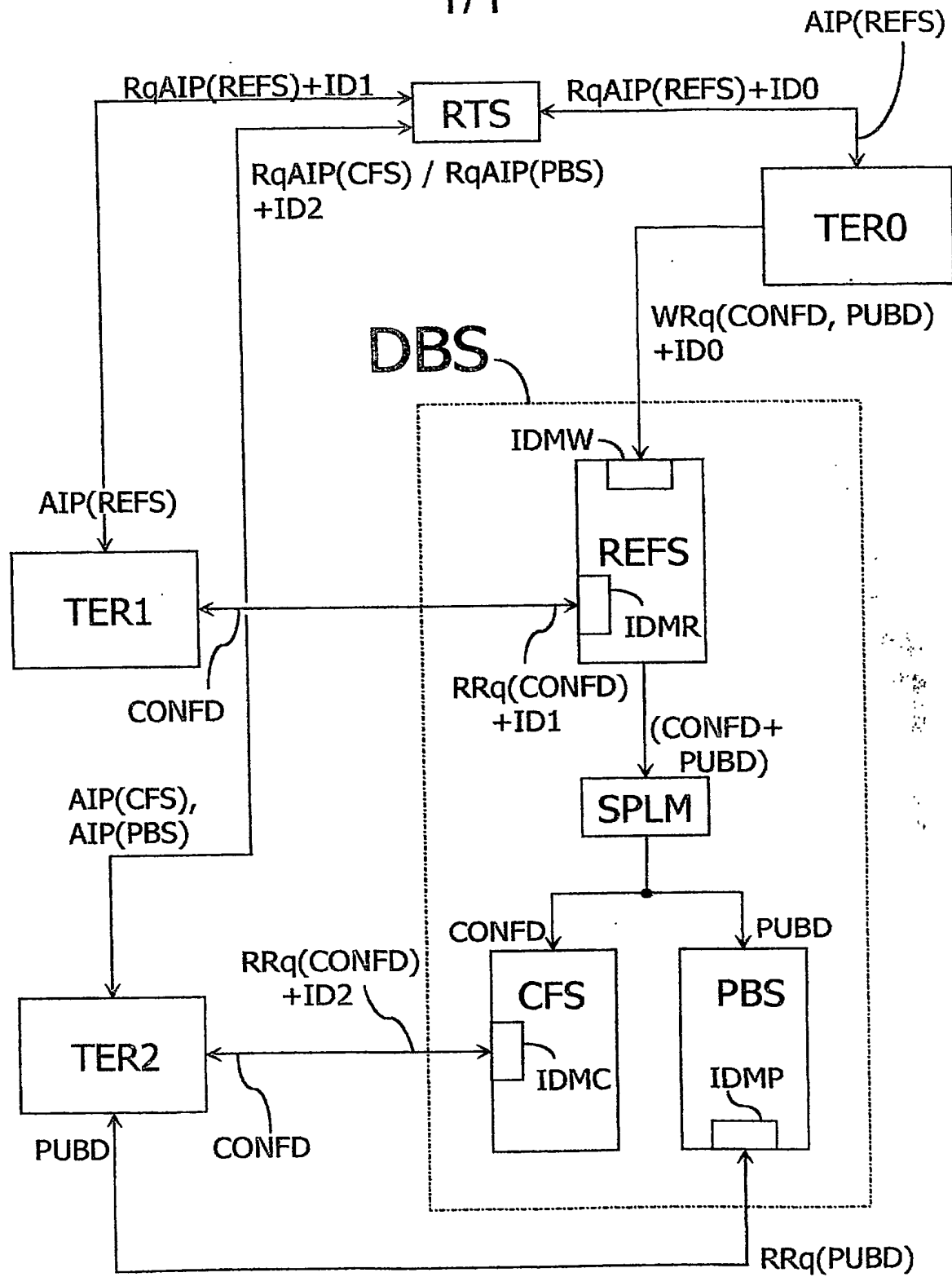


FIG.1



BREVET D'INVENTION

CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI



N° 11235*03

DÉPARTEMENT DES BREVETS

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08

Téléphone : 33 (1) 53 04 53 04 Télécopie : 33 (1) 42 94 86 54

DÉSIGNATION D'INVENTEUR(S) Page N° 1../1..

(À fournir dans le cas où les demandeurs et
les inventeurs ne sont pas les mêmes personnes)



Cet imprimé est à remplir lisiblement à l'encre noire

DB 113 @ W / 270601

Vos références pour ce dossier (facultatif)		10434
N° D'ENREGISTREMENT NATIONAL		0311350
TITRE DE L'INVENTION (200 caractères ou espaces maximum) Système de télécommunication mettant en oeuvre une résolution de noms de domaine sécurisée		
LE(S) DEMANDEUR(S) : FRANCE TELECOM S.A. 6, place d'Alleray 75015 PARIS		
DESIGNE(NT) EN TANT QU'INVENTEUR(S) :		
<input checked="" type="checkbox"/>	Nom	MIGAULT
	Prénoms	Daniel
Adresse	Rue	52, rue Hoche
	Code postal et ville	91213 ISSY LES MOULINEAUX
Société d'appartenance (facultatif)		
<input type="checkbox"/>	Nom	
	Prénoms	
Adresse	Rue	
	Code postal et ville	
Société d'appartenance (facultatif)		
<input type="checkbox"/>	Nom	
	Prénoms	
Adresse	Rue	
	Code postal et ville	
Société d'appartenance (facultatif)		
S'il y a plus de trois inventeurs, utilisez plusieurs formulaires. Indiquez en haut à droite le N° de la page suivi du nombre de pages.		
DATE ET SIGNATURE(S) DU (DES) DEMANDEUR(S) OU DU MANDATAIRE (Nom et qualité du signataire)		
SAINT-MARC Christophe 01-1000		

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

☐ **BLACK BORDERS**

☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**

☐ **FADED TEXT OR DRAWING**

☒ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**

☐ **SKEWED/SLANTED IMAGES**

☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**

☐ **GRAY SCALE DOCUMENTS**

☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**

☒ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**

☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.